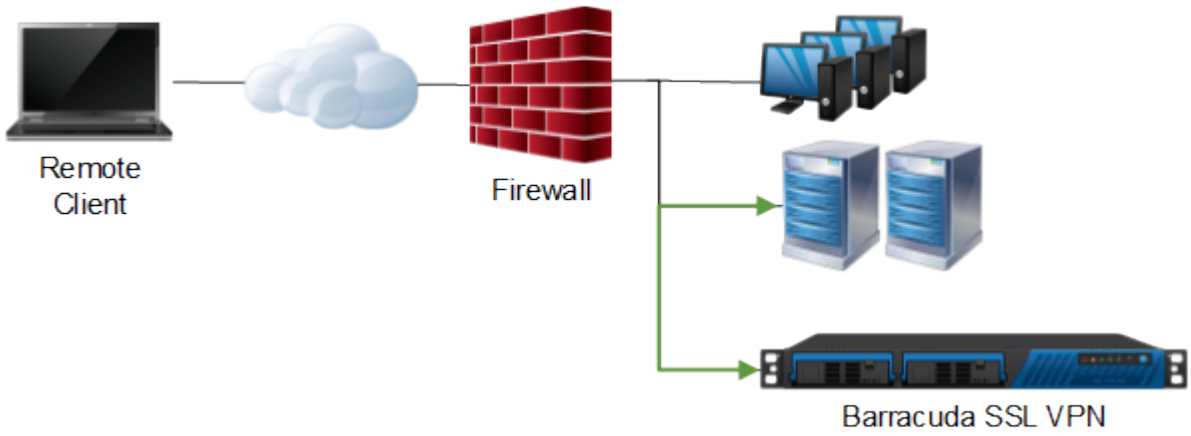
Deployment

https://campus.barracuda.com/doc/2458429/

The Barracuda SSL VPN is typically deployed in the following configurations:

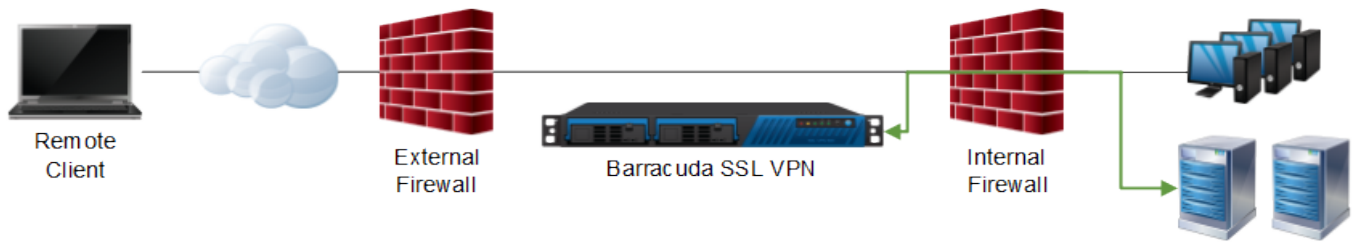
- **Direct Access Deployment** – Behind the firewall, with direct access to all intranet resources.
- **Multilayer Firewall DMZ Deployment** – In a DMZ between the external and internal firewall. Additional ports have to be opened on the internal firewall to access internal resources.
- **Isolated Deployment** – The Barracuda SSL VPN is reachable from the Internet. All resources connect via Server Agents which initiate the connection from inside the networks. No ports have to be opened.

Direct access deployment



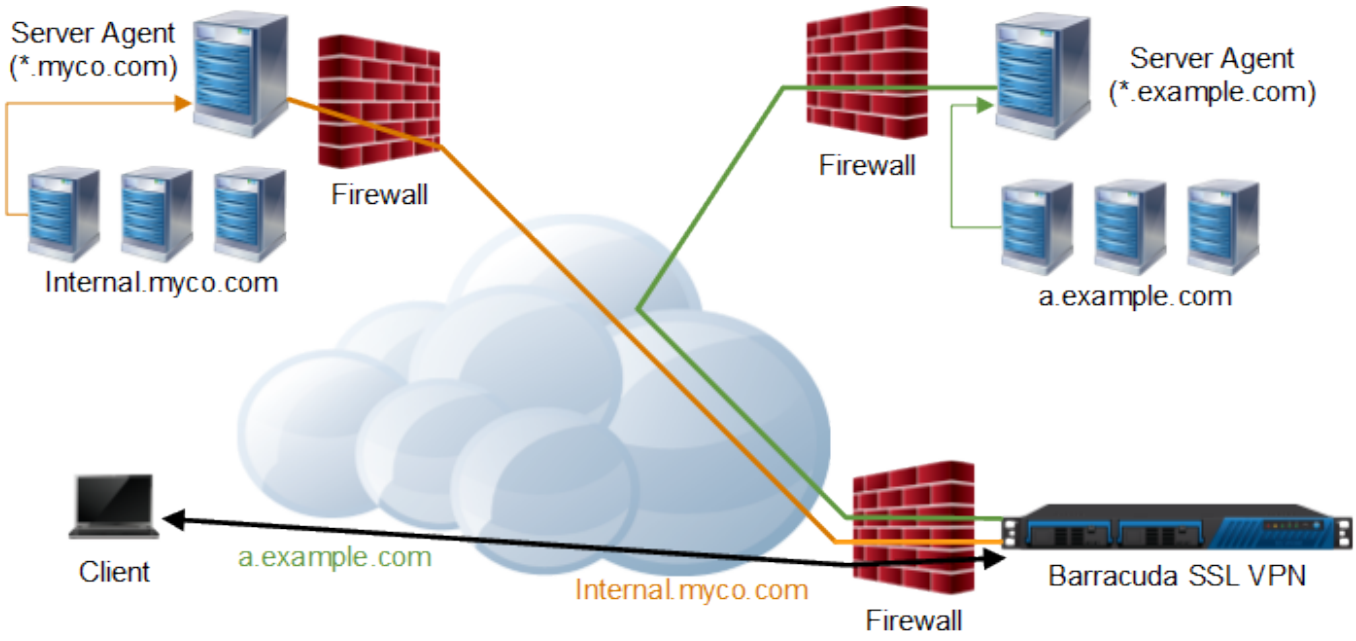
The Barracuda SSL VPN is deployed behind the firewall. Only one port (443) has to be opened up by the firewall and forwarded to the SSL VPN. You have direct access to all services (authentication, file, web, etc.) in the intranet without further configuration.

Multilayer firewall DMZ deployment



The Barracuda SSL VPN is deployed in a DMZ behind the corporate firewall but before the internal network firewall. All access to services on the internal network requires ports to be opened on the internal firewall. By deploying the Barracuda SSL VPN between the two firewalls, another security layer is added. It is also possible to install the Server Agent on a computer in the internal network, which initiates an SSL tunnel on port 443 from the inside of the network so you can limit the ports that you must open on the internal firewall.

Isolated deployment



The Barracuda SSL VPN is deployed and isolated from the rest of the network. All resources are located in networks which are not directly accessible by the Barracuda SSL VPN. Server Agents inside the networks initiate tunnels to the SSL VPN and act as proxies for the local resources. This deployment minimizes security implications caused by opening various ports on the firewalls to access the resources located behind them.

In this section

Figures